総務省（情報通信分野）の取組

資料２－４

■ サイバー攻撃への総合的な対応力の向上

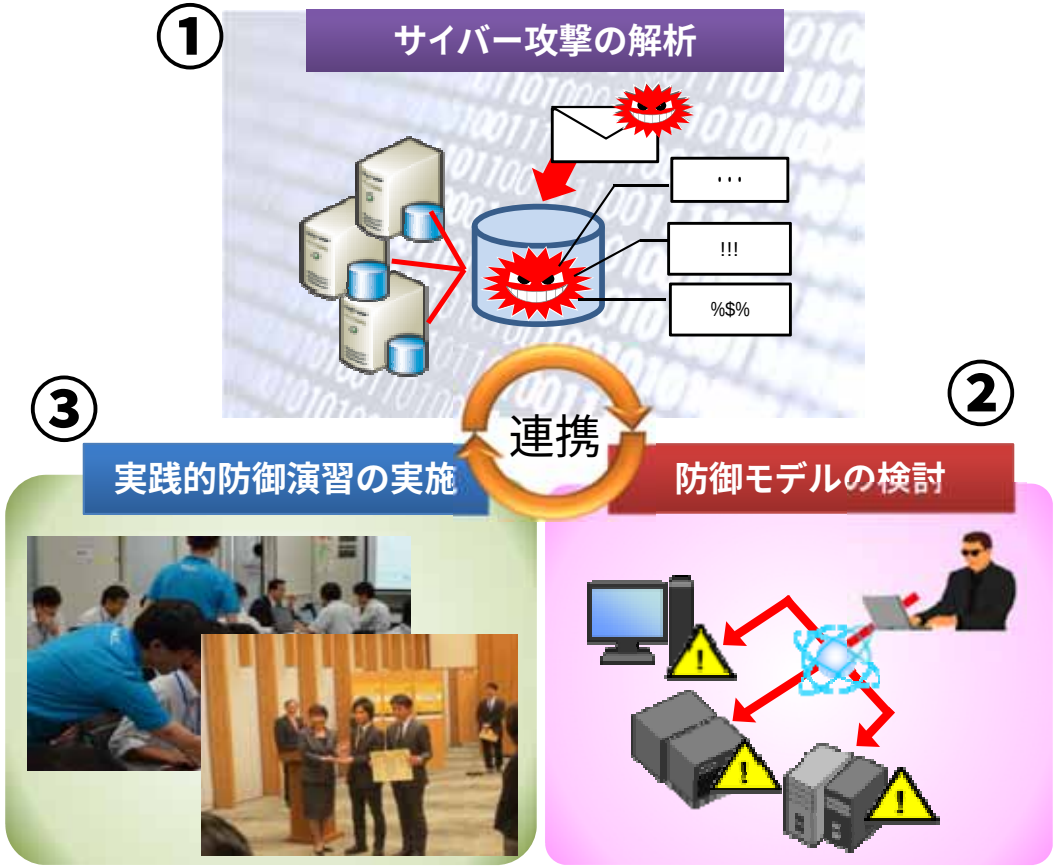
- **２０２０年東京オリンピック・パラリンピック競技大会を見据え、更に巧妙化・複合化するサイバー攻撃に備え、将来の我が国における安心・安全なサイバー空間を実現し、もって安全な社会経済基盤の実現を図るため、以下の取組を推進する。**
  - **① 実践的能力を有する人材の育成に向け、２０２０年東京大会関連システムの模擬も可能な大規模演習基盤を構築・運用するとともに組織の人材育成に対する支援を行う。**
  - **② サイバー攻撃や脆弱性等の情報を収集・解析し、ＩＳＰやセキュリティベンダ等の関係者間で共有することで、適切な対策を促す仕組みの構築・実証を行う。**
  - **③ 増大するＭ２Ｍ・ＩｏＴ機器の安全性の確保のため、セキュリティ技術開発や運用ガイドラインの策定等、当該機器への対策を促す仕組みの実証を行う。**

総務省（情報通信分野）の取組

■ サイバー攻撃複合防御モデル・実践演習

- **近年、巧妙化・複合化する標的型攻撃※について、攻撃の解析・防御モデルの検討及び実践的な防御演習を実施し、我が国における標的型攻撃に対する対処能力を向上させる。**

※特定の組織や個人を標的に複数の攻撃手法を組み合わせ、執拗かつ継続的に行われる攻撃。



大規模実証環境を活用し、以下の取組を推進する。

① サイバー攻撃の解析：
標的型攻撃の解析及び解析結果のデータベース化を通じ、標的型攻撃の特徴情報の体系化及び解析手法の確立を図る。

② サイバー攻撃防御モデルの検討：
①の結果を踏まえ、サイバー攻撃が発生した際のインシデントレスポンスについて検討を行い、防御モデルの確立を図る。

③ 実践的防御演習：
②で確立した防御モデルを踏まえ、官公庁・大企業等のLAN関係者を対象にしたサイバー攻撃への対応能力向上のための実践的防御演習を実施し、対処に必要なスキル項目の体系化を図る。